Using a Common Framework for Trusting Components in E-Authentication Systems

Workshop on

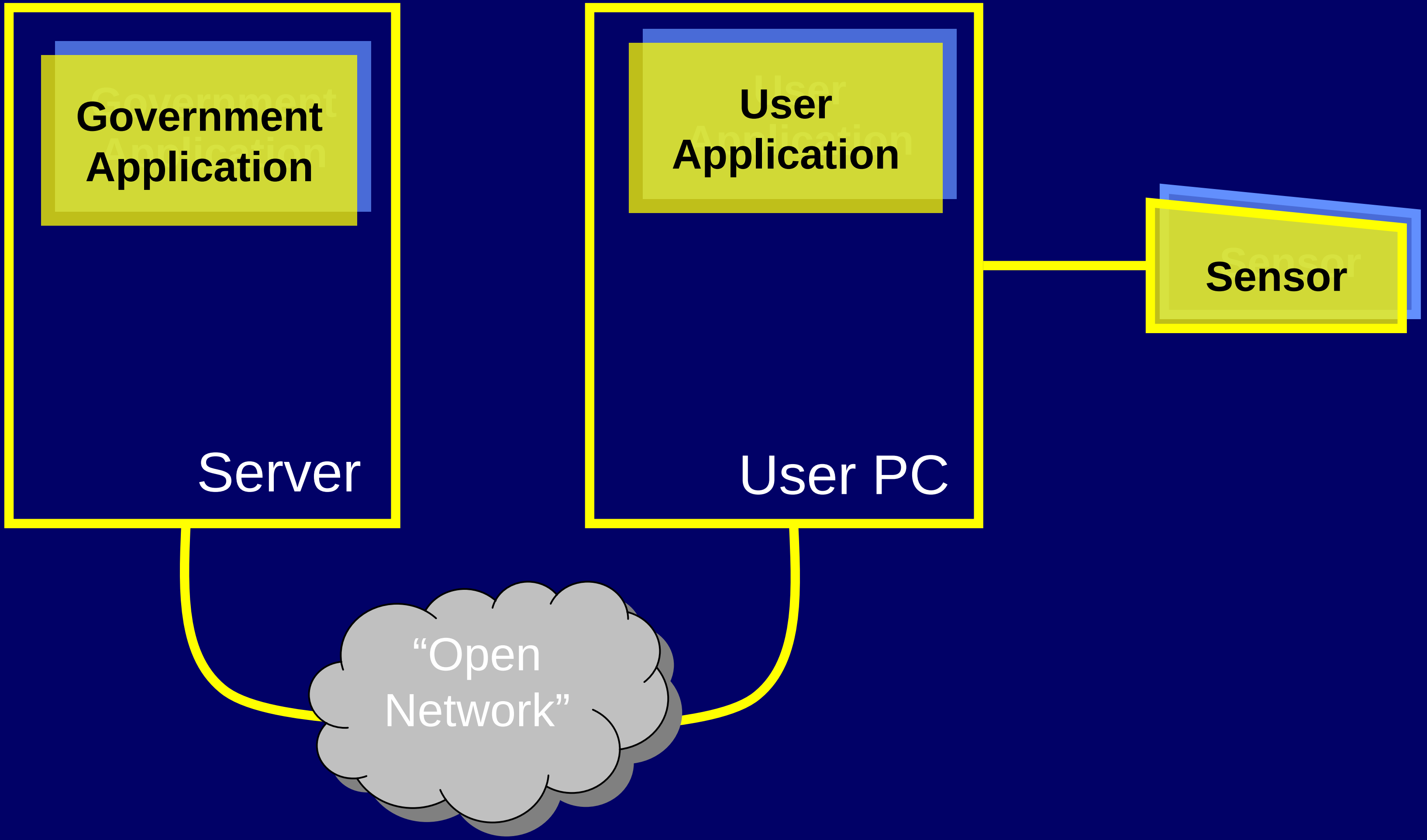
Biometrics and E- Authentication Over Open Networks

March 30th and 31st, 2005

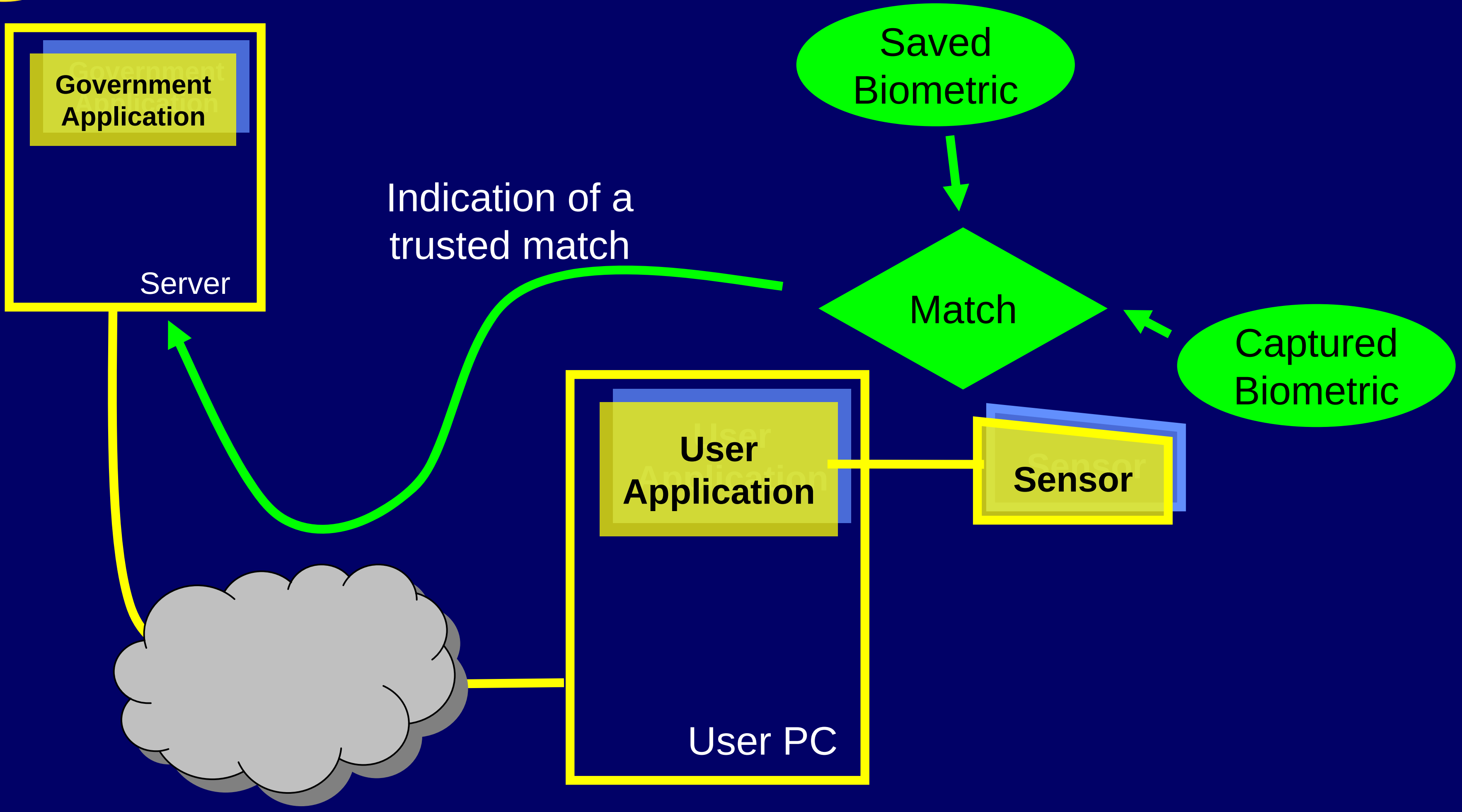
Authentication Over Open Networks

- **Biometric Enabled Identity Determination**
  - **match live sample to enrolled sample**
- **Application (Govt) needs to know result**
  - **an ID or**
  - **“there was a match”**
- **Match can be executed anyplace**
- **Goal is to trust the match result**
- **“level” of trust corresponds to OMB assurance levels (1-4)**

Biometric Enabled Identity Determination



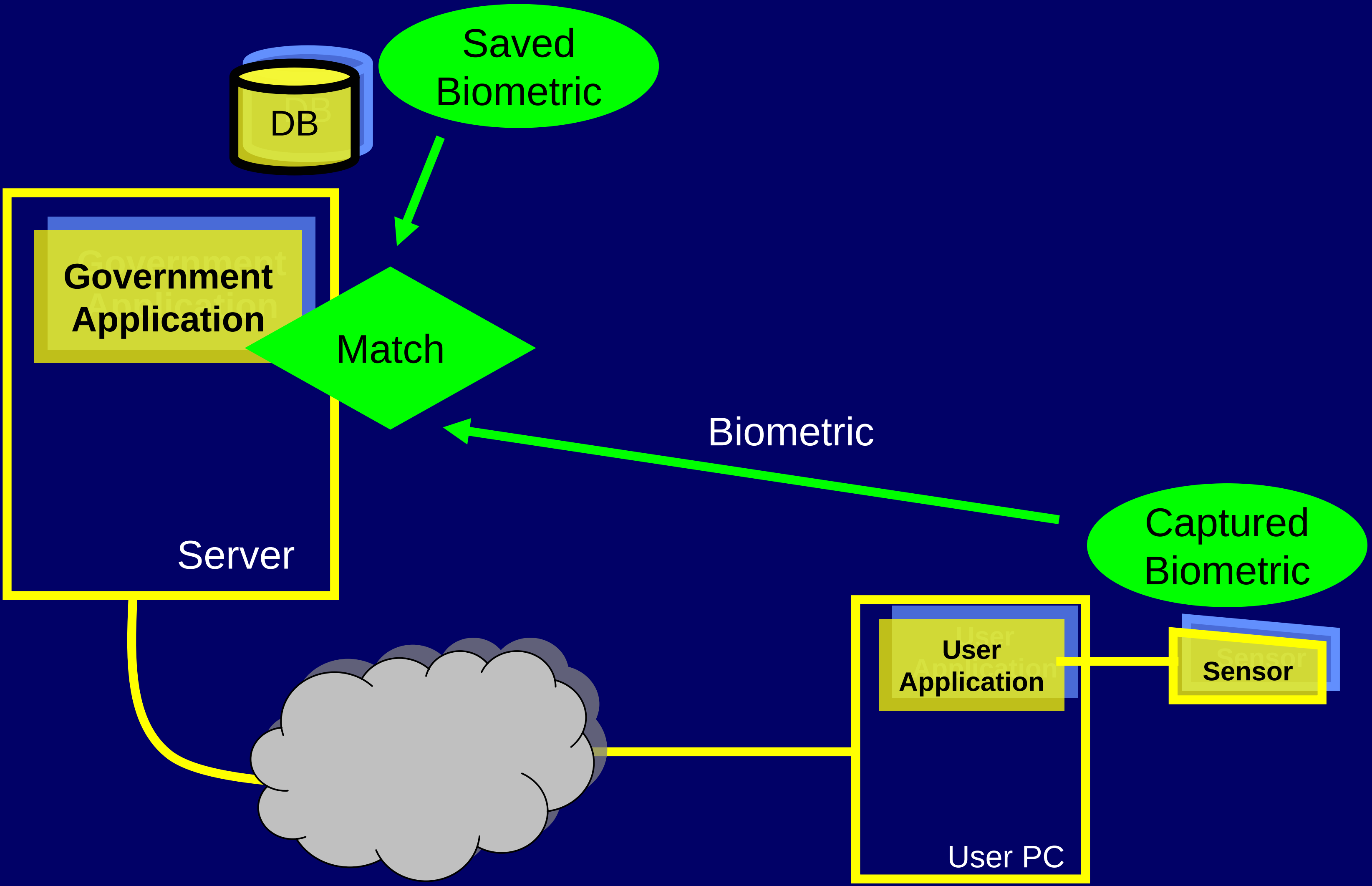
Match Off-Server



Traditional Data Security

(confidentiality, integrity, and source authentication)

Match On-Server



Trust the Biometric

Need to convey the biometric sample

- Trust the source
- Bind an identifier to the biometric
- Protect sensitive data
- Maintain integrity

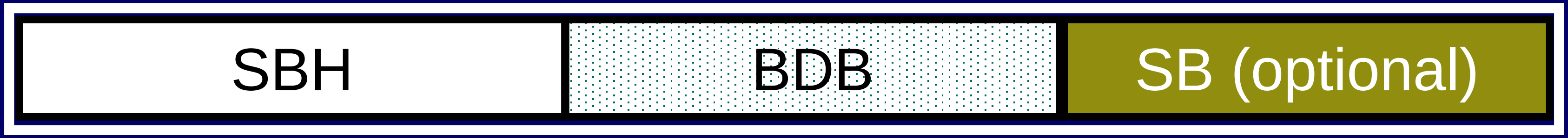
CBEFF

A framework of data communications and cryptography

- Ground rules and data requirements
- Multiple formats
- Common syntax
- Translation
- Interoperability

- Encoding in accordance with a CBEFF Patron Format
  - Full bit-level specification

CBEFF BIR



CBEFF specifies standard structures for *biometric information records* (BIRs)

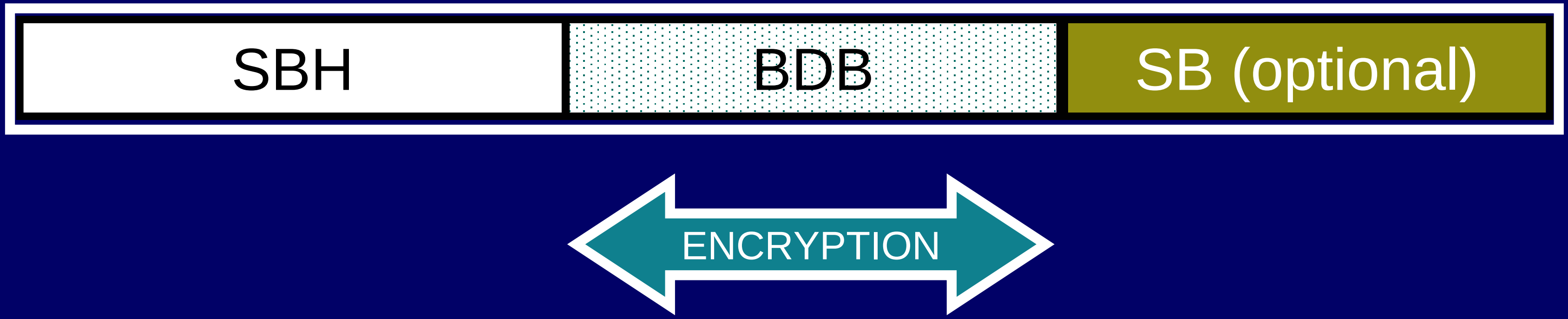
- **Standard Biometric Header (SBH)**
  - **Describes BDB**
- **Biometric Data Block (BDB)**
  - **Standard or proprietary**
  - **Registration process**
- **Signature Block (SB)**

Trust - Confidentiality

Encrypted BDB

- SBH has an indicator of BDB encryption
- Patron Format specifies encoding of
  - encryption algorithm
  - any necessary encryption parameters
- External key management

Encryption

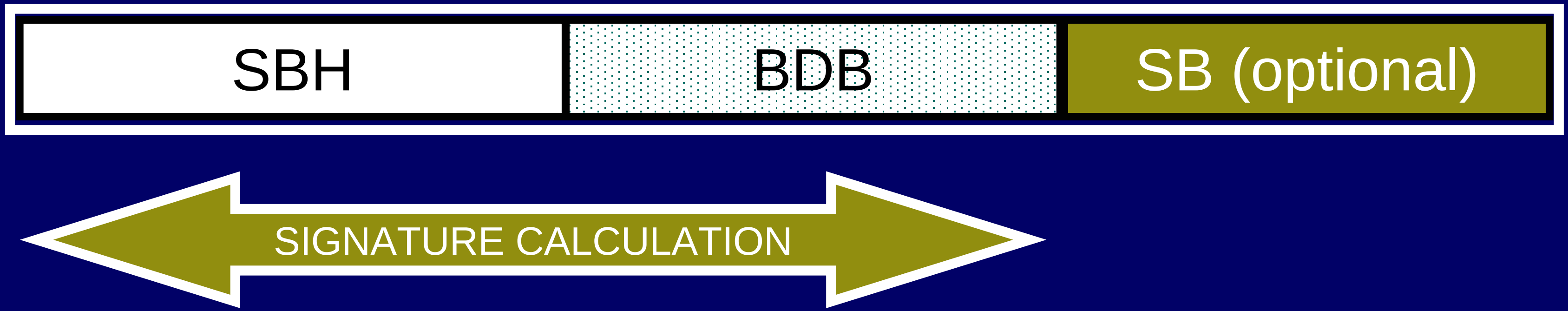


Trust - Integrity

Signature Block

- SBH has an indicator of presence of SB
- Patron Format specifies encoding of form and content of a signature block

Digital Signature



SBH

BDB

SB (optional)

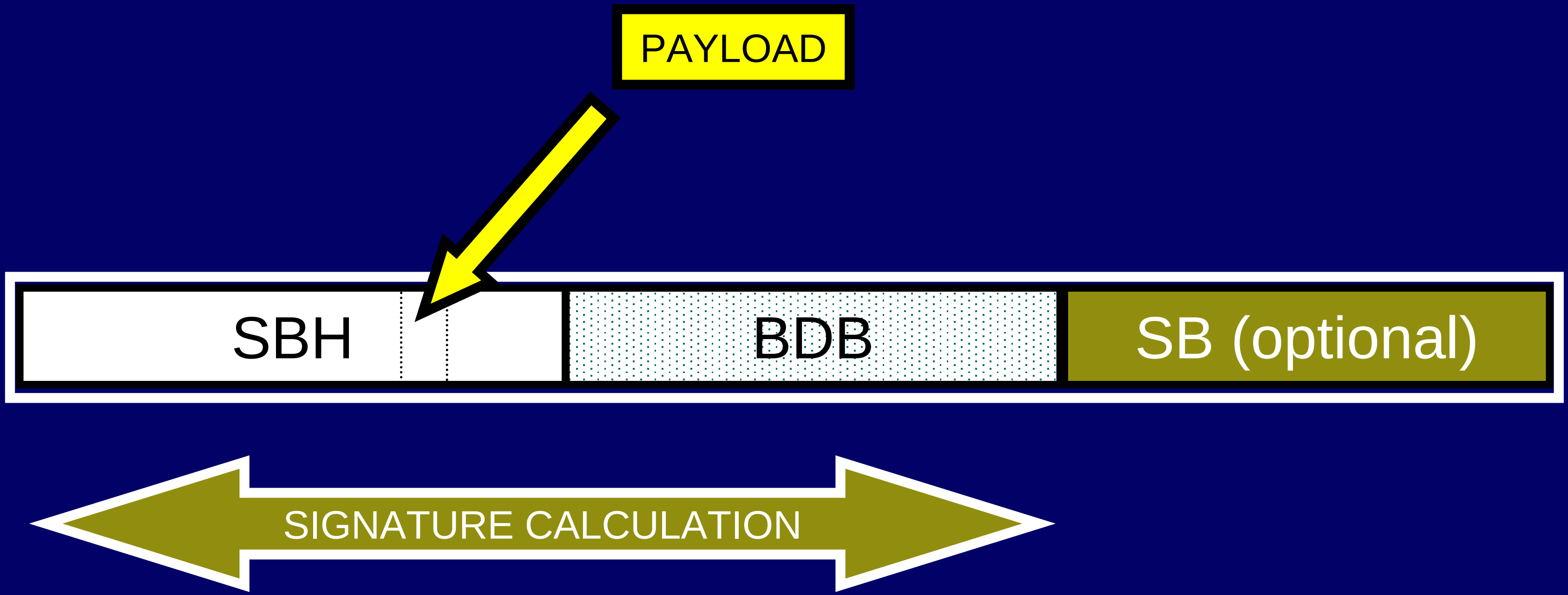
SIGNATURE CALCULATION

Trust – Binding Identity

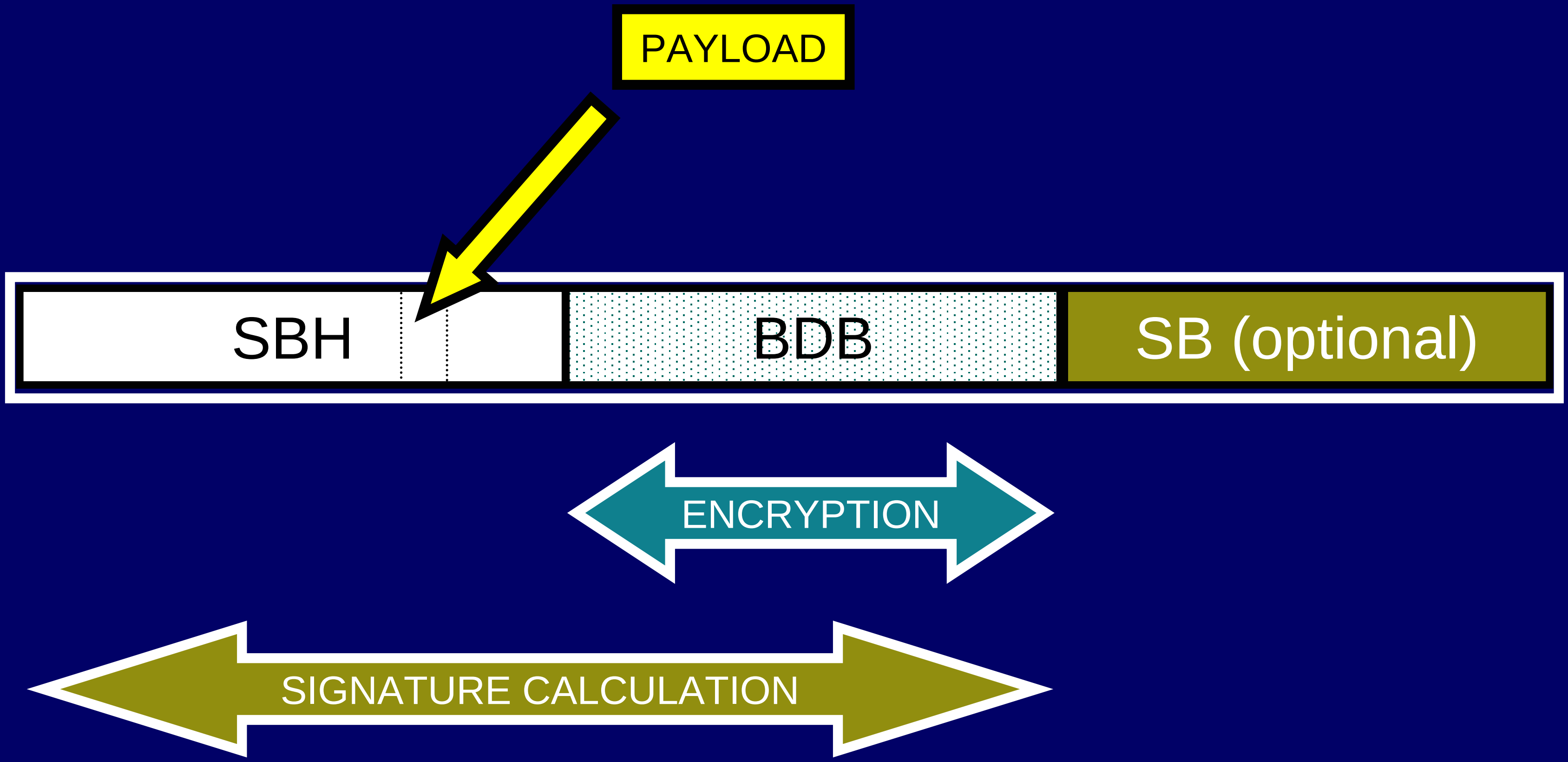
Payload

- Contained in SBH
- May contain arbitrary data
- Patron Format may specify identity data -- binding an identity to the biometric sample

Binding



Trust


PAYLOAD
SBH
BDB
SB (optional)
ENCRYPTION
SIGNATURE CALCULATION

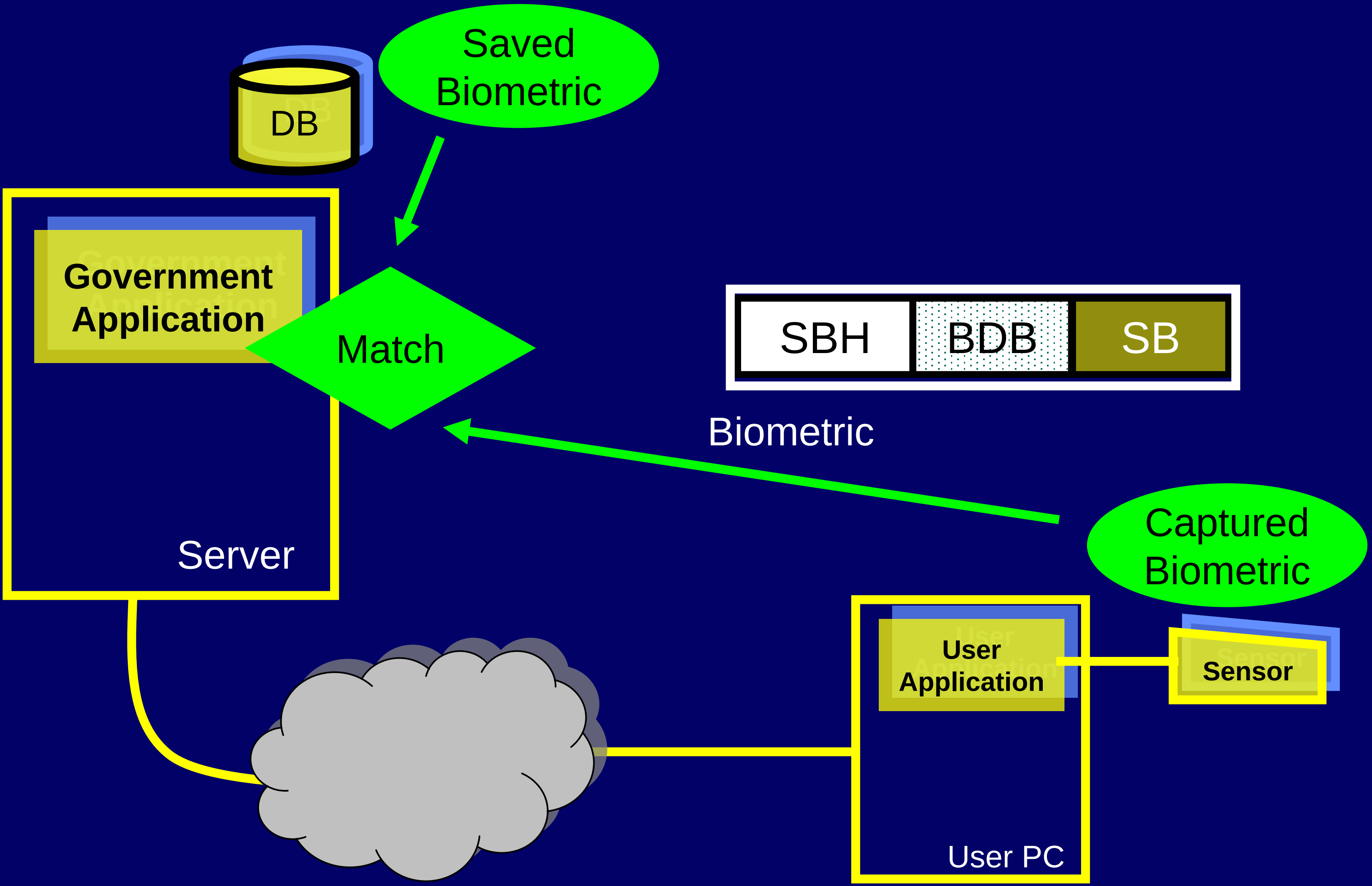
Patron Formats

- BioAPI Storage Format – Device Interface
- X9.84 – Financial Services
- ISO 7816-11 – Smart cards
- …others as needed

IBIA is Registration Authority

- New formats for new “Domain of Use”

Match On-Server



Contact Information

Dale Hapeman

Support Contractor

U.S. Department of Defense

Biometrics Management Office

304-326-3029

dale.hapeman@dodbfc.army.mil

www.biometrics.dod.mil